TREND MICRO™

Trend Micro
RISK INSIGHTS

Expose and prioritize risks for better decision making

Threat actors have become stealthier and more sophisticated, utilizing complex techniques to compromise devices and spoof identities. This allows criminals to spread attacks laterally throughout an organization's network to steal sensitive data and often demand a ransom for its retrieval.

Security is job zero

This changing threat landscape means that beginning your cyber health journey no longer begins and ends by simply installing a cybersecurity product. IT teams need to adopt a zero trust strategy. While there is "inherent trust" organizations instill on their architecture, zero trust prohibits attackers from piggybacking on that institutionalized trust.

Employing a zero trust strategy

This approach helps your IT teams thwart attackers by limiting access to resources and only allowing access via trusted, verified devices. Employing a zero trust strategy requires continuous and in-depth monitoring of devices and a sufficient level of identity health.

Addressing the needs of zero trust

As most modern access control solutions perform only cursory posture checks and only perform this duty during the initial connection, you require greater visibility and insight into risks to transform a "trust strategy" into a zero trust strategy.

Introducing Trend Micro Risk Insights

We understand the growing need for organizations to uncover and prioritize risks, that why we equip your security team with the ability to continually monitor your security posture. We help expose unseen risks so you can make better decisions. Across the organization, Risk Insights assists:

SOC/Security teams – Uncover undiscovered risks and gain insight into what needs immediate attention. View risks by user, device, and application, or at the organization level.

CSO/Leadership – Understand your organization's security posture, whether it is improving or declining, and gain visibility into how it compares to peers in your industry, region, or organization size.

Network security – Incorporate health scores into access control solutions and make more informed automated decisions when following a zero trust strategy.
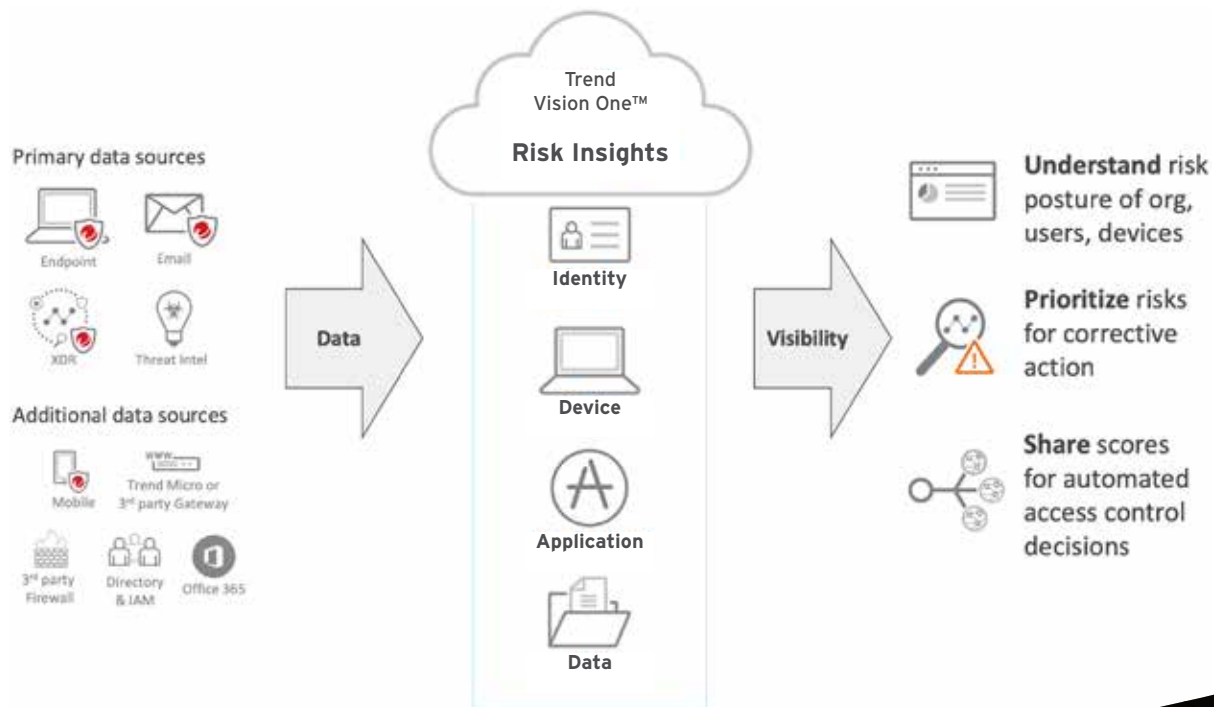
Increase visibility into threat and posture risks

- Provides continuous risk analysis of devices, identities, content, and applications. This includes active risks such as:
  - Suspicious or anomalous user activity
  - Indicators of attack (IoA), behaviors, or detections
  - Potential risks such as vulnerabilities, exposed identities, or risky cloud app access
- Allows for deeper insight into your organization's health level—pulled from endpoint, email, mobile, network XDR telemetry, and other data sources—to uncover hidden risks.
- Leverages intel from leading Trend Micro vulnerability research experts to detect unpatched operating system and application vulnerabilities within your environment
- Instills a zero trust strategy throughout your organization by providing your security team with continuous health assessments of your identities and devices.

Prioritization and automation for better risk-based decisions

- Highlights the most critical risks affecting your organization so your team can maintain a trusted security environment.
- Uses global and local exploit intelligence to prioritize patching of device vulnerabilities and identifies if prevention rules are available to protect against exploits until patch deployment.
- Mitigates and contains risks across the infrastructure from just one console.
- Shares health scores with Trend* and third-party access control solutions— including Trend Micro™ Zero Trust Network Access (ZTNA) and Trend Micro™ Secure Access Service Edge (SASE)—to make automated and well-informed decisions.

*Trend Micro Zero Trust Secure Access (ZTNA & SASE) is currently in preview
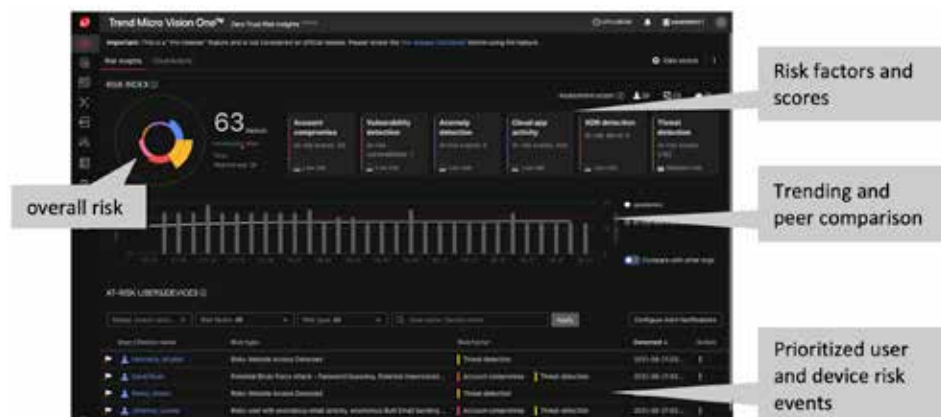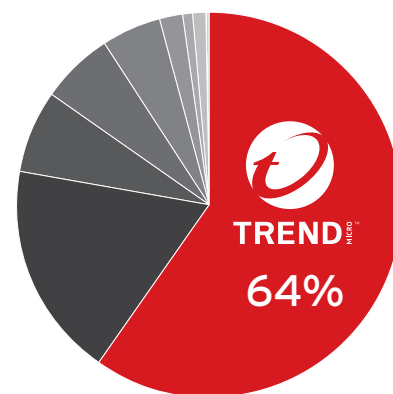
Trend Vision One™

Risk Insights is built on Trend Vision One, a powerful threat operations center that includes XDR, risk insights, and more, all designed to deliver confidence and efficiency to security operations staff.

Trend's leadership in vulnerability disclosure and threat research powers the vulnerability prioritization in Risk Insights.

Our 15 global research centers, 450 internal researchers, and over 10,000 external security researchers supporting our Zero Day Initiative™, provide visibility into the entire threat landscape. With teams dedicated to cloud and cloud-native applications, we use our wealth of knowledge to strengthen our products and protect your organization against current and future threats.

For more information, please visit **trendmicro.com**